UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
LUFKIN DIVISION

DEEP NINES, INC.

Plaintiff, Counter-Defendant

v.

MCAFEE, INC.

Defendant, Counter-Plaintiff.

9:06-CV-174-RC
JURY DEMANDED

PLAINTIFF DEEP NINES' REPLY MARKMAN BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES

I. INTRODUCTION

Deep Nines, Inc. (“Deep Nines”) accuses McAfee, Inc. (“McAfee”) of infringing U.S. Patent No. 7,058,976 (the ’976 patent”), entitled “Intelligent Feedback Loop Process Control System.” McAfee either adds limitations not supported by the intrinsic evidence or improperly downgrades the role of intrinsic evidence to serving as a check on the dictionary meaning of a claim term. In contrast, Deep Nines’ proposed constructions are consistent with the disclosure of the patentee, without improperly introducing unnecessary limitations into the claims. This brief sets forth Deep Nines’ rebuttal of McAfee’s Responsive Markman Brief.

II. CLAIM CONSTRUCTIONS OF DISPUTED CLAIM TERMS

The disputed terms of the ’976 patent are discussed below. The primary dispute between the parties is whether the claims cover the invention implemented on a broad variety of “gateways,” including individual computers connected to a network, as Deep Nines contends, or only on devices “connected to two or more different networks,” as McAfee asserts. Similarly, McAfee also attempts to limit the claimed inventions to protecting entire networks, as opposed to individual computers on a network. McAfee’s proposed constructions are inconsistent with the broader teaching of the ’976 patent, as discussed below.

A. (1) “Intercepting in real time the remaining data utilizing the intrusion detection system,” (2) “An intrusion detection system coupled to the firewall for intercepting in real time remaining data” and (3) “Passing remaining data to an intrusion detection system coupled to the firewall associated with the gateway”

Claim Term	Deep Nines’ Proposed Construction	McAfee’s Proposed Construction
“Intercepting in real time the remaining data utilizing the intrusion detection system” Claims 1 & 12	Intercepting in real time, all the data not discarded by the firewall utilizing the intrusion detection system.	Intercepting in real time the remaining data **before it gets to the network** utilizing the intrusion detection system.
“An intrusion detection system coupled to the firewall for intercepting in real time remaining data” Claims 7 & 13	An intrusion detection system **coupled in-line** with the firewall for intercepting in real time all the data not discarded by the firewall.	No constructions needed. Note, McAfee asserts that “intercepting in real time remaining data” means intercepting in real time the

Claim Term	Deep Nines' Proposed Construction	McAfee's Proposed Construction
"Passing remaining data to an intrusion detection system coupled to the firewall associated with the gateway" Claims 1 & 12	Passing remaining data to an intrusion detection system **coupled in-line** with the firewall associated with the gateway.	remaining data **before it gets to the network** utilizing the intrusion detection system.

The key dispute over the proposed construction of these terms is whether "intercepting in real time" or "passing" the "remaining data" from the firewall bears on the relationship between the firewall and the IDS, as Deep Nines contends, or if these actions occur "before it [remaining data] gets to the network," as urged by McAfee. McAfee's contention that the intrinsic evidence requires such a construction is plainly wrong.[1] Neither the claim language, the specification, nor the prosecution history supports this construction.

1. The Claims Are Properly Limited to In-line Coupling Between the Firewall and Intrusion Detection System

The parties dispute whether a person of ordinary skill in the art would understand "intrusion detection system coupled to the firewall" means an intrusion detection system (IDS) coupled in-line with the firewall, as Deep Nines contends. McAfee alleges that there is no support for this construction.[2]

While the plain language of the claims requires an "intrusion detection system coupled to the firewall" for "intercepting in real time" "remaining data," a person of ordinary skill in the art would not read the claim language in isolation, but in the context of the entire patent, including the specification and the prosecution history. *See Phillips*, 415 F.3d at 1313-14. The specification explains that "incoming packets are routed from . . . firewall 15, then go to detection/notification server 21 [IDS]"[3] of Figure 1. As apparent from this diagram, reproduced below, whatever packets are allowed to traverse firewall 15 by operation of the firewall rules are intercepted by the detection/notification server 21 (IDS) that is coupled in-line with firewall 15.

[1] *See* McAfee Responsive Markman Brief at 14-15.
[2] *See id.* at 18-21.
[3] '976 patent, col. 4, ll. 4-6; *see also* col. 4, ll. 42-55.

According to the Examiner, "[t]he applicant discussed what distinguishes the claimed invention over primary reference of Shipley is intercepting in real time before the intrusion gets to the protected network."[4] That is, Shipley[5] cannot intercept in real time an intrusion before the intrusion gets to what is being protected – network 20, as seen below in Fig. 1 from Shipley. In Shipley, whatever network traffic is allowed to traverse the firewall 18 is passed directly to network 20 and to INSD 10, the intrusion detection system, in parallel. Hence, even if Shipley's INSD detects an attack, it cannot be prevented because it will have already propagated across the network to one or more computers 14. Thus, the distinction made by the patentee between the "intercepting in real time" performed by the invention and Shipley was based on the relationship between the firewall and IDS in each system. In the '976 patent, because the "remaining data" from the firewall (firewall/proxy 15) is passed directly to the IDS (detection/notification server 21), it is not possible for an attack to bypass the IDS. In contrast, as seen in Fig. 1 from Shipley below, attacks always bypass the IDS (INSD 26), because it is only able to "monitor" or "capture" the "remaining data from firewall 18.

[4] Declaration of Alan Chen ("Chen Decl."), Exh. 1, '976 patent, Prosecution History, Interview Summary.
[5] Chen Decl., Exh. 2, U.S. Pat. No. 6,119,236 (filed Dec. 10, 1998).

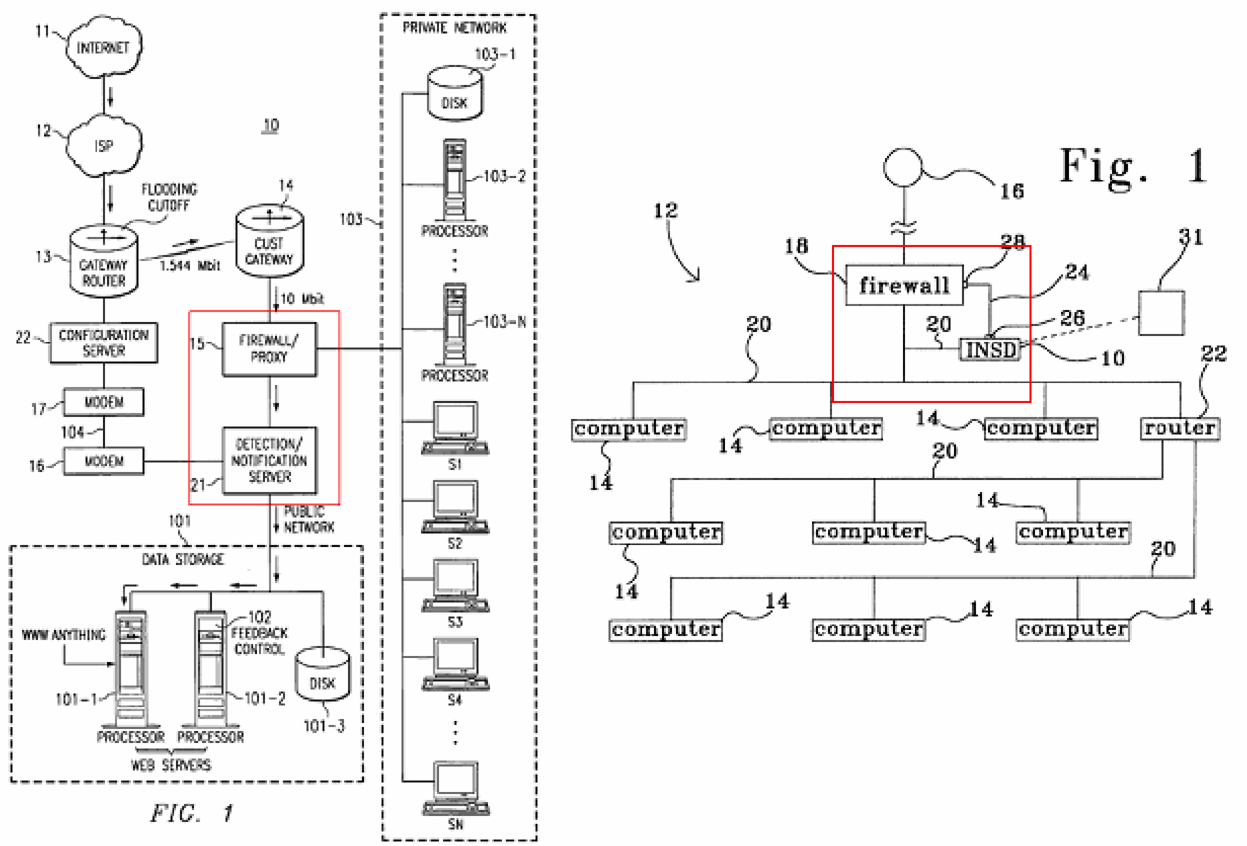
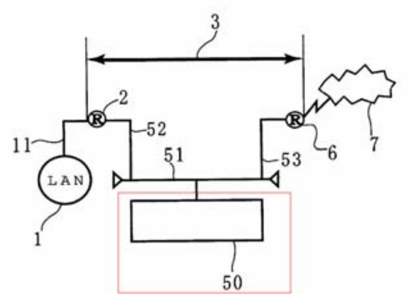


Fig. 1 of U.S. Patent No. 7,058,976 (L) and Fig. 1 of U.S. Patent No. 6,119,236 (R)

The prosecution history shows that the PTO and the Patentee understood intercepting in real time to exclude both mere monitoring and capturing:

> [S]hipley is silent in disclosing passing remaining data to the INDS [*i.e.*, IDS] and intercepting in real-time the remaining data utilizing the INDS and parsing the remaining data as recited in independent claims 75 and 81 [*i.e.*, issued claims 1 and 7]. Shipley's INDS dynamically reprograms the firewall to monitor the traffic whereas claims 75 and 81 require the intrusion detection system to be utilized in intercepting and parsing the remaining data passed to it.
>
> As per claims 86 and 87 [*i.e.*, issued claims 12 and 13], the closest prior art of record to (Gleichauf and Shipley) are silent in disclosing passing remaining data to the intrusion detection system and intercepting in real-time the remaining data utilizing the intrusion detection system and parsing the remaining data.

Chen Decl., Exh. 3, '976 patent, Prosecution History, Notice of Allowability, 3. Thus, "intercepting" cannot be interpreted to include monitoring schemes. Similarly, intrusion detection systems "capturing" (*i.e.*, "wiretapping") network traffic are not "intercepting" that traffic as in the ’976 invention. Both lack a firewall coupled in-line with an IDS. The following is an example of an IDS that captures (not intercepts) network packets:



Chen Decl., Exh. 4, U.S. Patent No. 6,263,444, Fig. 2 (the network unauthorized access analysis system 50 is shown in a “wiretap” configuration for capturing, rather than intercepting packets, transmitted between the buffering area networks 3). McAfee’s proposed constructions for these terms does not address the inventive relationship between the firewall and IDS, and is therefore inadequate.

2. McAfee’s “Before It Gets to the Network” Limitation is Improper

McAfee insists that the proposed constructions must include the limitation that the “remaining data” is intercepted “before it gets to the network.” Neither the specification nor the prosecution history requires such a limitation. Rather, the independent claims recite “intercepting in real time” “remaining data” from the firewall, not what follows the IDS. Indeed, the term “network” is not even a claim limitation; it appears nowhere in the body of the claims and is not limiting as preamble language, *infra*. Thus, the Examiner’s Interview Summary simply reinforces the plain and ordinary meaning of “intercepting in real time.” Besides finding no support from the claim language itself, *supra*, McAfee’s proposed construction also contradicts the specification. While the definition of the term “network” is not in dispute, the specification explicitly teaches that the invention can be used to prevent attacks to either (1) a network or (2) terminating devices connected to a network.[6] In fact, the specification describes in detail an embodiment of the invention “for operation with respect to a terminating device, or

[6] *See id.*, col. 8, ll. 62-65 (“[T]he concepts of this invention can be used at one or more network nodes or routing points along the network to help prevent attacks to either the network or to terminating devices connected to the network.”).

node, in a communication network," rather than the network itself.[7] As a "person of ordinary skill in the art is deemed to read the claim . . . in the context of the entire patent, including the specification," McAfee's proposed "network" limitation improperly limits the scope of the claimed invention. *See Phillips* v. *AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005); *Schriber-Schroth Co.* v. *Cleveland Trust Co.*, 311 U.S. 211, 217 (1940) ("The claims of a patent are always to be read or interpreted in light of its specification.").

3. Preamble Language Does Not Limit the Scope of the Asserted Claims

The disputed claim language – which is of course the starting point for determining the scope of a claim – makes no mention of any "network." Yet, McAfee contends that all of the claims require protecting a network against attacks,[8] because "the patentee purposefully and deliberately chose to draft claims specifically directed to protecting 'a network.'"[9] In support, McAfee cites to independent claims 1, 7, 12 and 13 of the '976 patent.[10] However, McAfee overlooks that the term "network" is <u>only</u> recited in the preamble—not in the body—of these claims. And even putting aside the fact that preamble language here is not limiting, McAfee's proposed construction is not supported by the plain language of the preambles that recite "<u>detecting</u> attacks on a network" rather than <u>protecting</u> a network.[11]

"Preamble language that merely states the purpose or intended use of an invention is generally not treated as limiting the scope of the claim." *Bicon, Inc. v. Straumann Co.*, 441 F.3d. 945, 952 (Fed. Cir. 2006). That is, where "the body of the claim 'sets out the complete invention,' the preamble is not ordinarily treated as limiting the scope of the claim." *Id.* at 952. In contrast, "when the limitations in the body of the claim 'rely upon and derive antecedent basis from the preamble, then the preamble may act as a necessary component of the claimed invention.'" *Id.*

[7] *Id.* at col. 8, ll. 60-62 ("[T]he invention has been described for operation with respect to a terminating device, or node, in a communication network . . . .").
[8] *See id.* at 3-4.
[9] *Id.* at 3; *see also id.* at 15-16.
[10] *Id.* at 3 n.11.
[11] '976 patent, claims 1, 7, 12 & 13 (emphasis added).

In this case, the preambles of claims 1, 7, 12 and 13 merely state the intended purpose of the claimed invention: "A method for detecting attacks on a network"[12] and "A gateway system for detecting attacks on a network."[13] And since the term "network" is only found in the preambles of claims 1, 7, 12 and 13, no limitations in the body rely upon and derive antecedent basis from the preamble. Therefore, the preamble language "detecting attacks on a network" does not limit the scope of the claims.

B. "Gateway"

Claim Term	Deep Nines' Proposed Construction	McAfee's Proposed Construction
"Gateway" Claims 1, 7, & 12-13[14]	An entrance and/or exit to a communications network.	A "gateway" connects two or more different networks.

The key dispute over this disputed term is the proper role of extrinsic evidence, especially dictionary definitions, in claim construction. Deep Nines' proposed construction focuses on the intrinsic evidence. In contrast, McAfee's undue reliance on dictionary definitions improperly downgrades the role of intrinsic evidence in claim construction to serving as a check on the dictionary meaning of a claim term. *See Phillips*, 415 F.3d at 1320 (criticizing dictionary focused approach taken in *Texas Digital Sys., Inc. v. Telegenix, Inc.*, 308 F.3d 1193 (Fed. Cir. 2002)).

McAfee's "heavy reliance on the dictionary divorced from the intrinsic evidence risks transforming the meaning of the claim term to the artisan into the meaning of the term in the abstract out of its particular context, which is the specification." *Phillips*, 415 F.3d at 1321. Even with technical dictionaries, "[t]here is no guarantee that a term is used in the same way . . . as it would be by the patentee." *Id.* at 1322.

[12] '976 patent, claims 1 & 12 (emphasis added).

[13] *Id.*, claims 7 & 13 (emphasis added).

[14] Note, "gateway" is not a limitation of claims 7 and 13, appearing only in the preambles of claims. *See Bicon*, 441 F.3d at 952 ("Preamble language that merely states the purpose or intended use of an invention is generally not treated as limiting the scope of the claim.") (citations omitted).

In this case, the Patentee has defined "gateway" by implication. *See Phillips*, 415 F.3d at 1321 (*quoting Vitronics*, 90 F.3d at 1582) (". . . the specification 'acts as a dictionary when it expressly defines terms used in the claims or when it defines terms by implication.'") (citations omitted). Claims 1 and 7 recite "[a] method for detecting attacks on a network, comprising: at a gateway, receiving data from a remote source which is destined for a target."[15] The specification mirrors the claim language, explicitly stating that the invention may be utilized at "one or more network nodes [*i.e.*, a device that is connected as part of a computer network] or routing points along the network to help prevent attacks to either the network or to terminating devices [*e.g.*, a computer or personal digital assistant] connected to the network."[16] Thus, "gateway" is a network node – *i.e.*, an entrance and/or exit to a communications network.

Not surprisingly, the prosecution history, which includes the prior art cited during the examination of the patent,[17] provides various examples where the meaning of "gateway" departs from McAfee's dictionary definition.[18] Taken together, the specification and prosecution history indicate that a "gateway" is an entrance and/or exit to a communications network.

Moreover, McAfee's narrow construction of "gateway" is inconsistent with its publicly-expressed belief <u>before</u> this lawsuit. McAfee revealed its true understanding of the scope of "gateway" by marking various products, accused of infringing the '976 patent, with the patent number of the McAfee patent lost in the interference between the parties, U.S. Patent No. 6,513,122.[19] Most of these products are intended for installation and use on stand-alone computers, which are "gateways" under Deep Nines' construction, but ironically, not McAfee's.

[15] '976 patent, claims 1 & 7 (emphasis added).

[16] '976 patent, col. 8, ll. 60-65 (emphasis added).

[17] *Phillips*, 415 F.3d at 1317 (*citing Autogiro*, 384 F.2d at 399) ("The prosecution history, which we have designated as part of the 'intrinsic evidence,' consists of the complete record of the proceedings before the PTO and includes the prior art cited during the examination of the patent."); *see also Acumed, LLC v Stryker Corp.*, 483 F.3d 800, 808 (Fed. Cir. 2007).

[18] *See* Deep Nines Opening Markman Brief at 22-23.

[19] *See, e.g.*, Chen Decl., Exh.. 5, Product Guide for McAfee Total Protection for Small Business, at D9-008076, 8082; Chen Decl., Exh. 6, Getting Started Guide for McAfee IntruShield IPS System, at D9-000007, 28-29.

Each of the claims in the ’122 patent refers to the term “gateway” in the same way as in the asserted claims of the ’976 patent.

C. “Target”

Claim Term	Deep Nines’ Proposed Construction	McAfee’s Proposed Construction
“Target” Claims 1, 7, 12 & 13	A process on a computing device for which the data is destined.	A network or terminating device on the network.

The key dispute is whether a person of ordinary skill in the art would recognize that a “target” means a process on a computing device for which the data is destined. McAfee alleges that such a person would understand “target” to merely mean a network or terminating device on the network.

The claim language itself provides the context of “data . . . destined for a target.”[20] Recalling the five conceptual layers of the TCP/IP Internet Protocol Suite (as an example), the target is defined in the Transport Layer so that data reaches its desired process (or application program).[21] A person of ordinary skill in the art would thus recognize that incoming data packets contain a destination port in the header for mapping the packets to a particular process running on a computer.[22] This is not just true of TCP/IP, but all network protocols that would be used with the invention.

The specification explains that the claimed invention can prevent attacks to either the network or to terminating devices connected to the network by intercepting in real time hostile data before it reaches its destination process:

> While the invention has been described for operation with respect to a terminating device, or node, in a communication network, the concepts of this invention can be used at one or more network nodes or routing points along the network to help prevent attacks to either the network or to terminating devices connected to the network.

[20] ’976 patent, claims 1, 7, 12 & 13.
[21] *See* Deep Nines Opening Markman Brief at 24.
[22] *See id*.

’976 patent, col. 8, ll. 60-65. Deep Nines agrees with McAfee that the target is a terminating, or computing, device on a network. Indeed, all network attacks are ultimately destined for a particular network application or process on one or more network devices on a network, as opposed to the network itself, which is comprised of copper or optical cables, or uses a wireless medium, to connect different nodes or devices on that network. Deep Nines’ proposed construction is not intended to cover any arbitrary process on the terminating device, but as the construction indicates, just the “process on a computing device for which the data is destined.” One of ordinary skill in the art would understand that attacks are made specifically to a particular network-aware process on a computing device. Thus, an ordinary artisan would understand “target” to mean a process on a computing device for which the data is destined.

D. “Wherein the data representing text identified as hostile is acted upon differently based on the type of the attack by at least one of blocking the data, alerting an administrator, and disconnecting the remote source”

Claim Term	Deep Nines’ Proposed Construction	McAfee’s Proposed Construction
“Wherein the data representing text identified as hostile is acted upon differently based on the type of the attack by at least one of blocking the data, alerting an administrator, and disconnecting the remote source” Claims 1, 7, 12 & 13	“Disconnecting the remote source” – terminating the connection between the remote source and the target (*i.e.*, blocking all data flow from the remote source). “Blocking the data” – Stopping the data representing text identified as hostile from reaching the target. “Remote source” – A process on a computing device that sends data to the target.	“Disconnecting the remote source” – terminating the connection to the remote source. “Blocking the data” – Stopping the data representing text identified as hostile from reaching the [protected] network. “Remote source” – a network or a terminating device on the network that sends data to the target.

This claim phrase can be broken into three sub-phrases each defined by the intrinsic evidence: “disconnecting the remote source,” “blocking the data,” and “remote source.” The key dispute over the term “blocking the data” is whether the data must be stopped before reaching the target, as Deep Nines proposes, or the [protected] network, as McAfee proposes. As an initial matter, Deep Nines objects to McAfee’s proposed construction as vague with regards to "[protected]." Regardless, the claims contain neither a "network" nor a "protected network" limitation.[23] In contrast, the claims plainly recite "receiving data from a remote source which is destined for a target." Therefore, "blocking the data" means stopping the data representing text identified as hostile from reaching the target.

The key dispute over the term "disconnecting the remote source" is whether "blocking all data flow from the remote source" effectively terminates the connection between the remote source and the target. McAfee alleges that there is no support for this construction as such a construction would blur the distinction between "blocking the data" and "disconnecting the remote source."[24] This is incorrect. Unlike "disconnecting the remote source," "blocking the data" blocks the particular data identified as hostile without necessarily disconnecting the remote source. The specification describes "blocking the data" as the "detection/notification server 21" (IDS) taking "appropriate action such as dropping the packet."[25] In contrast, the specification describes "disconnecting the remote source" as "detection/notification server 21" (IDS) taking "appropriate action such as . . . generating a command to the CCS process to block specific traffic,"[26] wherein the Concurrent Process Communication with Configuration Server(s) (CCS) "[c]hecks for the expiration of time on the 'block traffic' condition for various sources."[27] Thus, "disconnecting the remote source" means terminating the connection between the remote source and the target (*i.e.*, blocking all data flow from the remote source).

The dispute over the proposed construction of "remote source" is analogous to the dispute over the proposed construction for "target." The claim language itself provides the context of "receiving data from a remote source."[28] In fact, as McAfee points out in its Responsive Markman Brief, Deep Nines identified Internet 11 of Fig. 1 as written support.[29] A

[23] *See supra* Part II.A.
[24] *See* McAfee Responsive Markman Brief at 35-37.
[25] *See* '976 patent, col. 7, ll. 28-53 (emphasis added).
[26] *Id.*
[27] *See* '976 patent, col. 7, l. 64 – col. 8, l. 25 (emphases added).
[28] '976 patent, claims 1, 7, 12 & 13.
[29] McAfee Responsive Markman Brief, Exh. 4, 18 & 20; Exh. 10, 2; *see also* McAfee Responsive Markman Brief at 33.

person of ordinary skill in the art would recognize that a remote source is defined, *e.g.*, in the Transport Layer of TCP/IP – the Internet Protocol Suite[30] – so that a target can send a reply to the sending process (or application program).[31] Hence, "remote source" means a process on a computing device that sends data to the target.

E. Information gathering attacks

Claim Term	Deep Nines' Proposed Construction	McAfee's Proposed Construction
"Information gathering attacks" Claims 3, 10, 12 & 13	An attack on a network that collects information.	Attacks on the network that collect information without authorization.

The sole dispute over the proposed construction of this term is whether the claim term "information gathering attacks" requires the extraneous limitation "without authorization" as urged by McAfee. McAfee contends that the intrinsic evidence requires such a construction. Neither the claim language, the specification, nor the prosecution history, however, supports this construction.

Simply put, McAfee has not cited a single instance in which the claims, specification, or prosecution history describe "attacks" – let alone "information gathering attacks" – as being "unauthorized."[32] Moreover, McAfee's logic that "attacks" are by their nature "unauthorized"[33] is self-defeating. If an attack is inherently "unauthorized," then McAfee's construction merely adds superfluous language. Yet, by modifying "attack" with the limitation "without authorization," McAfee actually implies the existence of attacks with authorization.

And since the specification is silent with regards to "authorization," McAfee's construction needlessly adds uncertainty as to what constitutes "authorization." Is a network intruder or hacker who (a) enters a valid user identification and password or (b) connects utilizing publicly accessible computers or devices authorized to collect information from the

[30] *See* Deep Nines Opening Markman Brief at 2.
[31] *See id.* at 26.
[32] *See* McAfee Responsive Markman Brief at 37-38.
[33] *Id.*

network? Under Deep Nines' proposed construction (*i.e.*, an attack on a network that collects information), this inquiry is unnecessary. Whether a network is attacked with or without authorization does not change the fact that the network was attacked.

F. Acting on the data representing text identified as hostile

Claim Term	Deep Nines' Proposed Construction	McAfee's Proposed Construction
"An **intrusion detection system** coupled to the firewall for intercepting in real time remaining data, . . . ; and **acting on the data representing text identified as hostile in order to prevent an attack**, . . . , the **intrusion detection system** further capable of updating the predetermined list of data representing text associated with attacks." Claim 7 (emphases added)	"An **intrusion detection system** coupled to the firewall for intercepting in real time remaining data, . . . , and **acting on the data representing text identified as hostile in order to prevent an attack**, . . . , the **intrusion detection system** further capable of updating the predetermined list of data representing text associated with attacks."	*Indefinite* – Consists of a method step in an apparatus claim, which renders the claim indefinite as a matter of law.

The key dispute over the proposed construction of this term is whether a single typographical error – the usage of a semicolon rather than a comma – renders the term indefinite. McAfee alleges the claim is indefinite as a matter of law. The claim is amenable to construction, however, and the Court has authority to correct the typographical error through claim construction, *infra*.

"In the face of an allegation of indefiniteness, general principles of claim construction apply." *Datamize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1348 (Fed. Cir. 2005) (citation omitted). Except for the aforementioned typographical error, the intrinsic evidence unambiguously supports one and only one construction: the intrusion detection system acts on the data representing text identified as hostile. McAfee does not contend otherwise.

Preceding the disputed claim term, the claim recites an "intrusion detection system" for performing various tasks. And following the claim term, the claim recites the "intrusion detection system further capable of" performing another task. Thus, the context in which the disputed term is used supports only one interpretation: the “intrusion detection system” acts on the data representing text identified as hostile.

The usage of the disputed term in the other independent apparatus claim only reinforces this interpretation:

> [A]n **intrusion detection system** coupled to the firewall for intercepting in real time remaining data, . . . **,** and **acting on the data representing text identified as hostile in order to prevent an attack**, . . . , the **intrusion detection system** further capable of updating the predetermined list of data representing text associated with attacks;

’976 patent, claim 13 (emphases added). That is, claim 13 properly uses a comma rather than a semi-colon before the disputed claim term, thereby explicitly reciting the “intrusion detection system” acting on the data representing text identified as hostile. The claims themselves therefore preclude any reasonable debate that the error was anything but typographical. *See Phillips*, 415 F.3d at 1314 (even apart from the specification, the claims themselves provide substantial guidance as to the meaning of the disputed term).

Similarly, the specification explicitly teaches the “intrusion detection system” acting on the data representing text identified as hostile:

> Information packets come into the detection/notification server [an IDS] from firewall 15 via communication interface 210 and are intercepted by that interface and fed into microprocessor 211. Microprocessor 211 is at the same time loading programs from random access memory 212 which had been stored in disk storage 213. These programs are what logically intercept the incoming data within the random access memory. The programs operate to investigate the incoming data and to make determinations as whether to pass the data on without comment; pass the data on and perform other actions or block the data flow.

See, e.g., ’976 patent, col. 4, ll. 43-55. And as the prosecution history is silent with regard to the disputed claim term, the intrinsic evidence suggests no other interpretation.

McAfee has the burden of establishing by clear and convincing evidence that the claim is invalid as indefinite under 35 U.S.C. § 112, ¶ 2. *See Aero Prod.’s Int’l v. Intex Recreation Corp.*, 466 F.3d 1000, 1015-1016 (Fed. Cir. 2007); *see also Datamize*, 417 F.3d at 1347-48 (“‘By finding claims indefinite only if reasonable efforts at claim construction prove futile, we accord respect to the statutory presumption of validity and we protect the inventive contribution of patentees, even when the drafting of their patents has been less than ideal.'") (*quoting Exxon Research & Eng'g Co. v. United States*, 265 F.3d at 1371, 1375 (Fed. Cir. 2001)). McAfee has not met this burden.

McAfee's argument exalts syntactic and structural form over substance. The disputed claim term is clearly amenable to construction to a person of ordinary skill in the art and is therefore not indefinite. Moreover, the Court has the authority to correct the single typographical error – *i.e.*, the usage of a semicolon rather than a comma preceding the disputed term – as "the correction is not subject to reasonable debate based on consideration of the claim language and the specification" and "the prosecution history does not suggest a different interpretation of the claims." *Novo Indus., L.P. v. Micro Molds Corp.*, 350 F.3d 1348, 1354.

III. CONCLUSION

For the foregoing reasons and the reasons stated in Deep Nines' Opening Markman Brief, Deep Nines respectfully requests that the Court adopt Deep Nines' proposed claim constructions for the disputed and agreed terms of the '976 patent.

Respectfully submitted,

Dated: November 30, 2007

FISH & RICHARDSON P.C.

By: /s/ Barry K. Shelton
Thomas M. Melsheimer
txmelsheimer@fr.com
Texas Bar No. 13922550
M. Brett Johnson
mbjohnson@fr.com
Texas Bar No. 00790975
Decker A. Cammack
dmc@fr.com
Texas Bar No. 24036311
FISH & RICHARDSON P.C.
1717 Main Street
Suite 5000
Dallas, TX 75201
(214) 747-507 telephone
(214) 747-2901 facsimile

Barry K. Shelton
bks@fr.com
Texas Bar No. 24055029
Alan M. Chen
Texas Bar No. 24045646
Fish & Richardson P.C.
One Congress Plaza, Suite 810
111 Congress Avenue
Austin, TX 78701
(512) 472-5070 telephone
(512) 320-8935 facsimile

Robert M. Parker
rmparker@pbatyler.com
Texas Bar No. 15498000
Robert Christopher Bunt
rcbunt@pbatyler.com
Texas Bar No. 00787165
Charles Ainsworth
charley@pbatyler.com
Texas Bar No. 00783521
Parker & Bunt, Ainsworth, P.C.
100 E. Ferguson
Suite 1114
Tyler, Texas 75702
(903) 531-3535 telephone
(903) 533-9687 facsimile

Attorneys for Plaintiff
DEEP NINES, INC.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the above and foregoing document has been served on November 30, 2007 to all counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system per Local Rule CV-5(a)(3). Any other counsel of record will be served by electronic mail.

Martin Rose
Michael D. Richardson
Rose-Walker, L.L.P.
3500 Maple Avenue
Suite 900
Dallas, Texas 75219

Attorneys for Defendant
McAfee, Inc.

Danny L. Williams, Esq.
J. Mike Amerson
Ruben S. Bains
Williams, Morgan & Amerson, P.C.
10333 Richmond - Suite 1100
Houston, TX 77042

Attorneys for Defendant
McAfee, Inc.

J. Thad Heartfield
The Heartfield Law Firm
2195 Dowlen Road
Beaumont, TX 77706

Attorneys for Defendant
McAfee, Inc.

Keith A. Rutherford
Wong, Cabello, Lutsch, Rutherford &
Brucculeri, L.L.P.
20333 SH 249, Suite 600
Houston, Texas 77070

Attorneys for Defendant
McAfee, Inc.

/s/ Barry K. Shelton
Barry K. Shelton